Estimations on the Security Aspect of Brand's Electronic Cash Scheme

Chang Yu Cheng*, Jasmy Yunus*, and Kamaruzzaman Seman**
*Faculty of Electrical Engineering,
Universiti Teknologi Malaysia,
81300 Skudai, Johor, Malaysia.
E-Mails: cyu_cheng@bip.utm.my, jasmy@bip.utm.my

**Telekom R&D,
UPM-MTDC Incubation Center,
Lebuh Silikon,
Universiti Putra Malaysia,
43409 Serdang,
Selangor, Malaysia.
E-Mail: drkzaman@rndtm.net.myE-mail

Abstract

In Crypto'93, Stefan Brands [1] proposed a very efficient off-line electronic cash. Then, the subsequent researchers such as Ernest Foo [2,3], WK Yip [4] and Yiannis [5] developed their schemes based upon Brands model [1] to improve Brand's efficiency. In this paper, we demonstrate the feasibility of attacks on Brands scheme's security aspect. By our attacks presented here, we conclude the security aspect of [1,2,3,4,5] has been defeated by us. Although we address here that Brand's security aspect need to be further investigated, but the anonymous feature in Brand's scheme [1] remain significant contributions to electronic cash, especially for privacy reason.

Keywords: *Electronic Payment Systems, Cryptography, Network Security, Electronic Cash, Brands model.*

1. Introduction

In Crypto'93, Brands presented a very efficient off-line electronic cash scheme based on the representation problem in groups of prime order [1]. Subsequently, the efficiency of [1] is improved further by Ernest Foo [2,3], WK Yip [4] and Yiannis [5], with the underneath security of their schemes remain as [1]. In this paper, we discover flaws of [1], that are applicable also to [2,3,4,5]. We however, have also perform fix on the security of Brands [1] in our another paper at [6]. Hence, we believe that the original contributions of Brands in [1] and in [2,3,4,5] are strong and represent important electronic cash systems to be further studied and improved.

Our counterfeit attacks in this paper include sequential attacks and parallel attack. *Sequential attack* is that attack that the attacker interacts sequentially with the signer. While *Parallel Attack* is the attack which the attacker can initiate several interactions at the same time with the signer in any order she wants. Our attacks enable the attacker(s) to spend their withdrawn coin more than once, without being detected. This is done in such a way that the User, *U* can mint the coin parameters satisfy the verification equations of the coin signature, even if she does not know the Bank's private key.

Organization: The purpose of this paper is to investigate on the security aspect of [1]. In Section 2, we will estimate on the security of [1] and discuss our attacks on [1]. We then conclude this paper in Section 3.

2. Security estimations and attacks on Brands scheme

In this section, we show how the fraudulent user can successfully perform various counterfeit attacks on Brands scheme [1]. The details descriptions of Brands scheme kindly refer to [1]. We exploit the weakness of the security aspect of Brands [1] by performing sequential and parallel attacks. The fix of these attacks

Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05)
1550-445X/05 $20.00 © 2005 **IEEE**

over Brands scheme is further discussed in our paper at [6].

2.1. Counterfeit Attacks

Proposition 1. *Fraudulent users can counterfeit/forge a coin in Brand's wallet with observer model. Any schemes based upon the security of Brand's model are vulnerable to this form of attacks.*

Proof:

[Attack 1]

The attack here is to reinvent the user part of the payment protocol, in such a way that the user does not require carrying out the related withdrawal protocol. This means the user can mint the coin by herself and spend such coin at Shop, *S*. With such modified fraudulent payment protocol in Brand's model, anyone can forge the coin, because User, *U* can make the coin parameters satisfy the verification equations, even if she does not know *B*'s private key.

Note that $g_1^{r_1} g_2^{r_2} = A^d B$

Let $r_{1i} = r_1' + w_1 d + x_1 \bmod q$

$\overset{(*)}{=} eo_1 + o_2 + w_1 d + x_{1i} \bmod q$

(Let $d'=e$)

Let $r_{2i} = d + x_2 \bmod q$

Thus $g_1^{r_1} g_2^{r_2} = g_1^{eo_1 + o_2 + w_1 d + x_1} g_2^{d + x_2}$

$\overset{(*)}{=} A_o^e B_o (g_1^{w_1} g_2)^d (g_1^{x_1} g_2^{x_2})$

(Let $A = g_1^{w_1} g_2$, $B = g_1^{x_1} g_2^{x_2} A_0^e B_0$)

$= A^d B$

Now, we assume the fraudulent user forge *z',a',b,'r'* too. This means, the fraudulent user can forge the whole coin.

Then $g^{r'} = g^{w_2 + w_3 c'}$

$\overset{(*)}{=} h^{c'} a'$

(Let $h = g^{w_3}$, $a' = g^{w_2}$)

From $A^{r'} = z'^{c'} b'$

$(g_1^{w_1 w_2} g_2^{w_2})(g_1^{w_1 w_3} g_2^{w_3})^{c'} \overset{(*)}{=} z'^{c'} b'$

(Where $z' = g_1^{w_1 w_3} g_2^{w_3}$, $b' = g_1^{w_1 w_2} g_2^{w_2}$). The result above is shown in Figure 1.

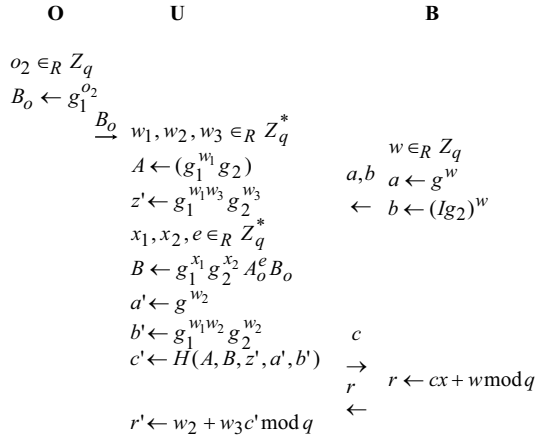

Figure 1: Attack 1: Withdrawal protocol of attacked Brand's model

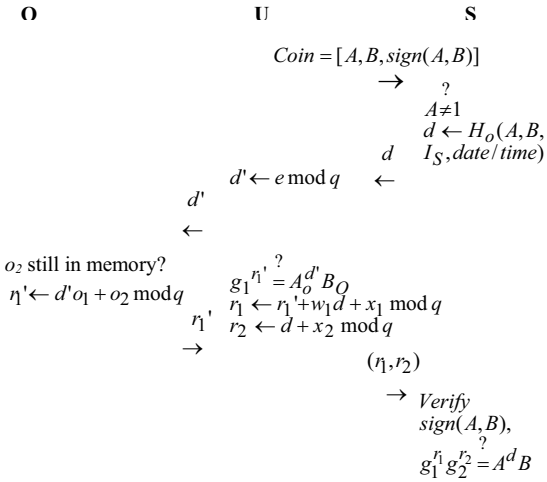

Figure 2: Attack 1: Payment Protocol of attacked Brand's model

Note that, if user double spent in deposit, the information the Bank, *B* have is the pair (r_1, r_2, d) and (r_1*, r_2*, d*). Thus the Bank, *B* tries to compute the user's identity, as below:

$$r_1 = r_1' + w_1 d + x_1 \bmod q$$
$$\overset{(*)}{=} eo_1 + o_2 + w_1 d + x_1 \bmod q$$
$$r_{1i}^* = eo_1 + o_2 + w_1 d^* + x_1 \bmod q$$
$$r_{2i} = d + x_2 \bmod q$$
$$r_{2i}^* = d^* + x_2 \bmod q$$
$$\left(\frac{r_1 - r_1^*}{r_2 - r_2^*}\right) = \frac{w_1 (d - d^*)}{d - d^*} = w_1,$$

However, this is not user's identity. Thus, the User, *U* can double spend without her real identity being revealed. Bank, *B* cannot determine the double spender even if she spends the forged coins multiple times.

[Attack 2]

This attack is another type of parallel attack. In this parallel attack, two users join force to compute a coin. This computed coin does not go through withdrawal protocol. Firstly, each of the two users withdraws a coin. Then, they compute and fake the third coin by themselves using such withdrawn information. When the user uses that third coin, the Bank cannot trace double spender. This indicates that, this third coin is in fact a valid coin/extra coin, generated by the user. We provide the following proof for the attack.

Based on the Brand's model, let

$a^* = g^{w^*}, a^{**} = g^{w^{**}}, r^* = c^* x + w^* \bmod q,$
$r^{**} = c^{**} x + w^{**} \bmod q$

Also, let $r' = (\beta r^* + \gamma r^{**})u + v \bmod q$

Thus, from $g^{r'} = h^{c'} a'$,

$$\Rightarrow a' = g^{r'} h^{-c'}$$
$$= g^{(\beta r^* + \gamma r^{**})u + v} h^{-c'}$$
$$\overset{(*)}{=} g^{\beta c^* ux + \beta w^* u + \gamma c^{**} ux + \gamma w^{**} u + v} h^{-c'}$$

(From $\beta c^* u + \gamma c^{**} u = c' \quad \Rightarrow \quad \beta c^* + \gamma c^{**} = c'/u$)

So, $a' = g^{\beta c^* ux + \beta w^* u + \gamma c^{**} ux + \gamma w^{**} u + v} g^{-(\beta c^* u + \gamma c^{**} u)x}$

$$\overset{(*)}{=} a^{*\beta u} a^{**\gamma u} g^v$$

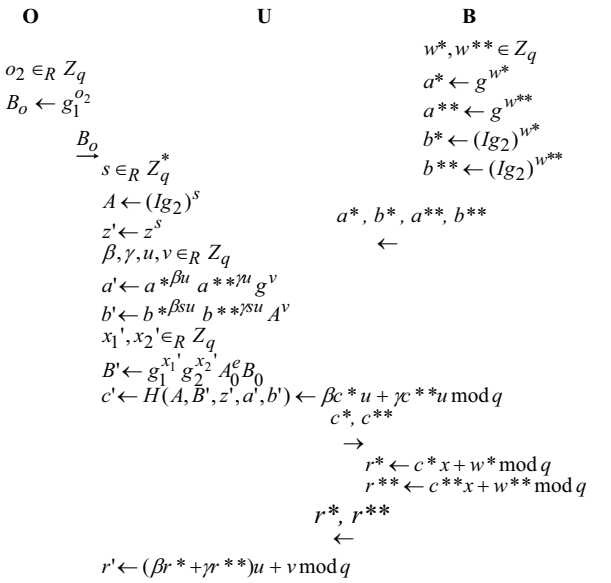

Figure 3 Withdrawal protocol for Attack 4 on Brand's Model

From $A^{r'} = z'^{c'} b'$

$$\Rightarrow b' = A^{r'} z'^{-c'}$$
$$\Rightarrow b' = [(Ig_2)^s]^{(\beta r^* + \gamma r^{**})u + v} [(Ig_2)^{sx}]^{-c'}$$
$$\overset{(*)}{=} [(Ig_2)^{w^*}]^{\beta su} [(Ig_2)^{w^{**}}]^{\gamma su} [(Ig_2)]^{sv}$$
$$\therefore b' = b^{*\beta su} \; b^{**\gamma su} A^v$$

This means, for the new coin,

$g^{r'} = h^{c'} a'$, where,

$r' = (\beta r^* + \gamma r^{**})u + v \bmod q, \mathrm{c}' = (\beta \mathrm{c}^* + \gamma \mathrm{c}^{**})\mathrm{u} \bmod \mathrm{q}$,

$a' = a^{*\beta u} \; a^{**\gamma u} g^v$

Also, $A^{r'} = z'^{c'} b'$, *where*, $\mathrm{b}' = \mathrm{b}^{*\beta \mathrm{su}} \; b^{**\gamma su} A^v$

This means that, the two users, which each perform a withdrawal protocol, can use the information get from withdrawal protocol to fake another extra coin, and spend it without being identified. Figure 3 shows the withdrawal protocol of the Attack 2 on Brand's model.

Figure 3 shows the withdrawal protocol for Attack 2 carried out on Brand's model. Note that,

$$c' = (\beta c^* + \gamma c^{**})u \bmod q = H(A, B' z', a', b'),$$

where $B' = g_1^{x_1'} g_2^{x_2'} A_0^e B_0$.

$$g_1^{r_1} g_2^{r_2} = A^d B$$
$$\overset{(*)}{=} g_1^{sd(o_1 + u_1) + x_1' + o_1 e + o_2} g_2^{sd + x_2'}$$

Thus,

$$r_1 = sd(o_1 + u_1) + x_1' + o_1 e + o_2 \bmod q$$
$$\overset{(*)}{=} [d' o_1 + o_2] + d(u_1 s) + x_1' \bmod q$$
$$= r_1' + d(u_1 s) + x_1' \bmod q$$

Also $r_2 = sd + x_2' \bmod q$

Thus, the fraudulent user chooses suitable x_1', x_2'. So,

$$r_1 = do_1 s + du_1 s + x_1' + eo_1 + o_2 \bmod q$$
$$r_2 = ds + x_2' \bmod q$$

When Bank want to detect double spender, the Bank check from its database of the previous coin with

$$r_1^* = d^* o_1 s + d^* u_1 s + x_1' + eo_1 + o_2 \bmod q$$
$$r_2 = d^* s + x_2' \bmod q$$

Thus

$$\Rightarrow \frac{r_1 - r_1^*}{r_2 - r_2^*} = \frac{s(o_1 + u_1)(d - d^*) + (x_1' - x_1)}{(d - d^*)s + (x_2' - x_2)} \neq o_1 + u_1$$

Thus, the fraudulent user's identity cannot be traced, when the fraudulent user performs double spending.

[Attack 3]

Here, we show that Brand's model is vulnerable to so-called "parallel attacks", in which two users perform their withdrawals in parallel, and then frame up a coin with cooperation. This attack enables two users to obtain a coin that contain neither of their identities. They are able to spend more than once using

such counterfeit coin. The magic in this attack is to find suitable value of μ, u_A, u_B, s_A, s_B, w_A, w_B in order the user can spend the fake coin multiple times. Now, we suppose that two users U_A and U_B perform the withdrawal scheme in parallel. Note that, each user is using their withdrawal information separately. First, the user U_A and U_B sends c_A and c_B to Bank, B. The B sends back r_A and r_B to U_A and U_B separately. These two users compute: $c' = \mu c_A' + c_B' \bmod q$ (where $c_A' = 2u\mu c_A \bmod q, c_B' = 2uc_B \bmod q$), $a = (a_A^{\mu} a_B)$, $r = \mu r_A + r_B \bmod q$.

Let $A_i = (g_1^{u_i} g_2)^{s_i}$ (where $i = A, B$),

And $c' = \mu c_A' + c_B' \bmod q$

From $g^{r'} = h^{c'} a'$, $a' = g^{r'} h^{-c'}$, and

$$a' = a^u g^v = g^{r'} h^{-c'}$$

Note that

$$a' = a^u g^v = (a_A^{\mu} a_B)^u g^v = (g^{w_A \mu} g^{w_B})^u g^v$$
$$= g^{\mu w_A u + u w_B + v} \quad (1)$$

(We assign:

$$r_A = c_A x + w_A \bmod q, r_B = c_B x + w_B \bmod q,$$
$$r' = (\mu r_A + r_B)u + v \bmod q, c_A = \frac{c_A'}{2u\mu} \bmod q,$$
$$c_B = \frac{c_B'}{2u} \bmod q)$$

From $a' = g^{r'} h^{-c'}$

$$= g^{(\mu r_A + r_B)u + v} h^{(\mu c_A' + c_B')}$$
$$\overset{(*)}{=} a' g^{\mu c_A ux + c_B ux - \mu^2 2uc_A x - 2uc_B x}$$

(Substitute from (1))

$$\therefore a' = a' g^{\mu c_A ux + c_B ux - \mu^2 2uc_A x - 2uc_B x}$$
$$\Rightarrow 1 = g^{\mu c_A ux + c_B ux - \mu^2 2uc_A x - 2uc_B x}$$

This means that,

$$\mu c_A ux + c_B ux - \mu^2 2uc_A x - 2uc_B x = 0$$
$$\overset{(*)}{\Rightarrow} ux[(\mu c_A + c_B) - 2(\mu^2 c_A + c_B)] = 0$$

Since $u \neq 0, x \neq 0$, thus:

$$(\mu c_A + c_B) - 2(\mu^2 c_A + c_B) = 0$$
$$\overset{(*)}{\Rightarrow} (2c_A)\mu^2 - c_A \mu + c_B = 0 \quad (2)$$

$$\therefore \mu = \frac{-c_A \pm \sqrt{c_A^2 - 4(2c_A)c_B}}{2(2c_A)} = \frac{-c_A \pm \sqrt{c_A^2 - 8c_A c_B}}{4c_A}$$

This attack is done, as the user calculates the value of μ. Thus, Brand's model is vulnerable to all our attacks. This proof is complete. □

3. Conclusions

This paper's objective is to identify the security flaw exist in Brand's scheme [1]. Such "breaking" also apply to [2,3,4,5] schemes, as they are based upon [1]. We have also performed fix on these attacks in [6], thus enabling further usage of [1,2,3,4,5] if some modifications based on our fix in [6] is performed. Thus, we believe that the original contributions in [1,2,3,4,5] are strong and important too.

4. Acknowledgements

We would like to thank Universiti Teknologi Malaysia and Mr. Goh Chu Leong for funding the project.

5. References

1. Stefan Brands. Untraceable off-line cash in wallets with observers. *In Advances in Cryptology, Crypto'93, Proceeding (Lecturer Notes in Computer Science 773)*: Springer Verlag. 1993. 302-318.

2. Colin Boyd, Ernest Foo, and Chris Pavlovski. Efficient Electronic Cash Using Batch Signatures. *ACISP'99, (Lecturer Notes in Computer Science 1587)* : Springer-Verlag, Berlin Heidelberg. 1999. 244-257.

3. Ernest Foo. *Strategies for Designing Efficient Electronic Payment Schemes.* PhD thesis. Queensland University of Technology, Australia; August 2000.

4. A.Goh, WK Yip. A Divisible Extension of the Brands Digital Cash Protocol: K-Term Coins Implemented via Secret Sharing. *TENCON 2000* : IEEE. 2000.

5. A.Chan, Y.Frankel, and Yiannis Tsiounis. Easy Come-Easy Go Divisible Cash. *In Advances in Cryptology-Proceedings of Eurocrypt'98, volume 1403 (Lecturer Notes in Computer Science).* May 1998 : Springer-Verlag. 1998. 561-575.

6. Chang Yu Cheng, Jasmy Yunus, Kamaruzzaman Seman. JCK Scheme-Secure Divisible Cash. To be submitted for proceeding of Eurocrypt (Lecturer Notes in Computer Science). Springer-Verlag.